

# PROCÉDURE DE DEPLOIEMENT DE SNORT SUR PFSENSE

**Auteur** : Maxime GILLE

**Reference** : Assumer

**Date** : 07/04/2023



	Titre	Reference	Page	
	Mise en place de SNORT sur PFSENSE	Assumer	2 / 8	

## DIFFUSION et VISAS

Diffusion				
Société / Entité	Destinataires	Fonction	Diffusion	Pour info
Assumer	Service IT	Procédure	Réseau	

Visas			
Société/Entité	Nom	Fonction	

## SUIVI DES VERSIONS

Version	Date	Auteur	Raison	Nombre de pages
V1.0	07/04/2023	Maxime GILLE	Procédure d'installation de SNORT sur PFSENSE	8

## COORDONNEES

Contacts		
Nom	E-mail	Téléphone
Maxime GILLE	maxime.gille@edu.esiee-it.fr	06.43.09.98.54

	Titre	Reference	Page	
	Mise en place de SNORT sur PFSENSE	<b>Assurmer</b>	3 / 8	

# Table des matières

1. Topologie réseaux de SNORT page 4

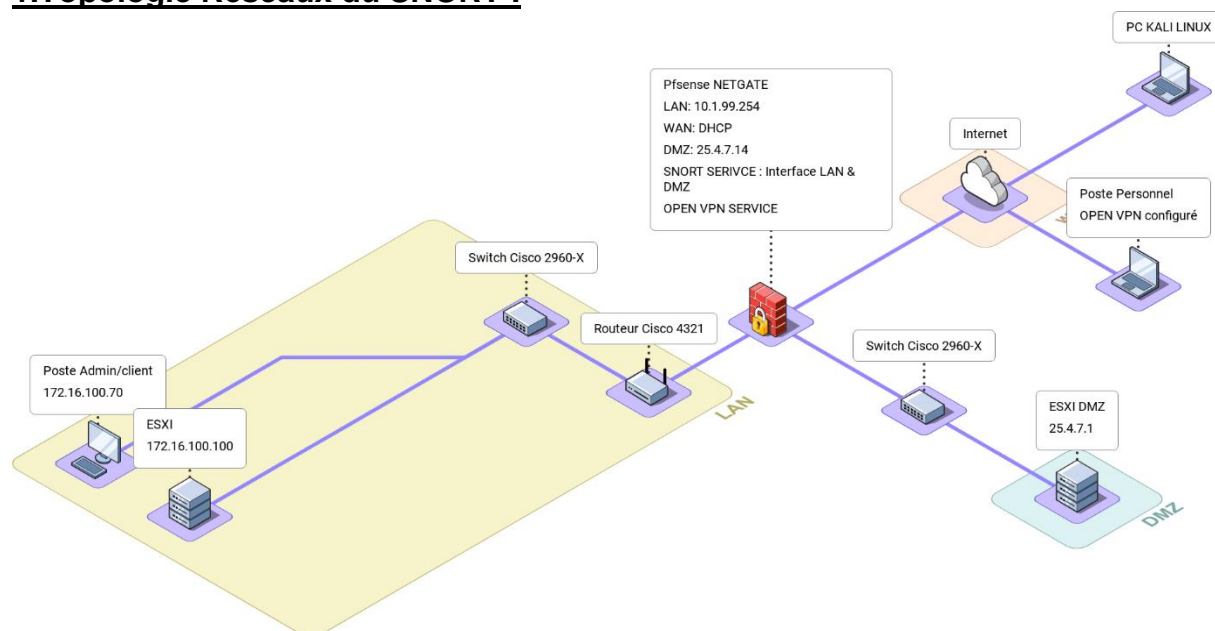
2. Configuration de la solution SNORT

-Installation de SNORT page 4

-Configuration de SNORT page 5

	Titre	Reference	Page	
	Mise en place de SNORT sur PFSENSE	Assumer	4 / 8	

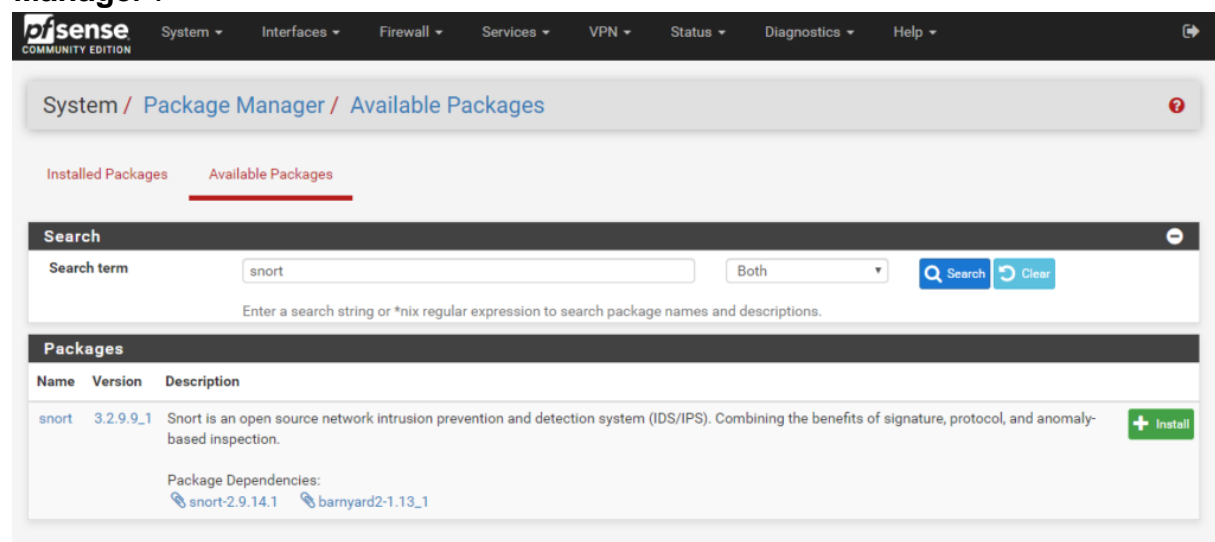
## 1.Topologie Réseaux du SNORT :



## 2.Configuration de la Solution SNORT :

### Installation de SNORT :

Une fois notre **PFSENSE** installé et configuré, nous nous rendons dans le **Packet Manager** :



	Titre	Reference	Page	
	Mise en place de SNORT sur PFSENSE	Assumer	5 / 8	

On clique ensuite sur **Install** puis **Confirm** et l'installation se lance ! Rien de très compliqué donc.

### Configuration de SNORT :

Une fois installé, Snort apparaîtra dans l'onglet **Services**. Une fois rendu dessus, nous allons dans un premier temps aller sur l'onglet **Global Settings** :

The screenshot shows the 'Global Settings' page for Snort in pfSense. The page is organized into several sections, each with an 'Enable' checkbox and a description:

- Snort Subscriber Rules:** Includes 'Enable Snort VRT' with a checkbox and links to sign up for a free or paid account.
- Snort GPLv2 Community Rules:** Includes 'Enable Snort GPLv2' with a checkbox and a description of the community ruleset.
- Emerging Threats (ET) Rules:** Includes 'Enable ET Open' and 'Enable ET Pro' with checkboxes and links to sign up for an ETPro account.
- Sourcefire OpenAppID Detectors:** Includes 'Enable OpenAppID' with a checkbox and a description of the OpenAppID package.
- OpenAppID Version:** A section for the OpenAppID version.
- Enable RULES OpenAppID:** Includes a checkbox and a note about the AppID Open Rules file.

La première étape est donc d'activer le téléchargement de règles gratuites, en cochant la première case (**Enable Snort VRT**). Il faudra renseigner une clé et pour l'obtenir il vous faudra créer un compte sur le site officiel de Snort.

Et ensuite nous pouvons cocher les cases :

- **Enable Snort GPLv2**, pour les règles communautaires ;
- **Enable ET Open**, qui sont des règles proposées par la société ET ;
- **Enable OpenAppID**, éventuellement, qui est une autre société ;

Et ensuite, pour les derniers paramètres il convient simplement de configurer l'update pour les différentes règles, c'est-à-dire le délai avant de vérifier les mises à jour pour les différentes règles ou pour de nouvelles :

	Titre	Reference	Page	
	Mise en place de SNORT sur PFSENSE	Assumer	6 / 8	

### Rules Update Settings

Update Interval

12 HOURS

Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Update Start Time

01:00

Enter the rule update start time in 24-hour format (HH:MM). Default is 00:05. Rules will update at the interval chosen above starting at the time specified here. For example, using the default start time of 00:05 and choosing 12 Hours for the interval, the rules will update at 00:05 and 12:05 each day.

Hide Deprecated Rules Categories

☐ Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

Disable SSL Peer Verification

☐ Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

### General Settings

Remove Blocked Hosts Interval

NEVER

Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.

Remove Blocked Hosts After Deinstall

☐ Click to clear all blocked hosts added by Snort when removing the package.

Keep Snort Settings After Deinstall

☒ Click to retain Snort settings after package removal.

Startup/Shutdown Logging

☐ Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

Save

Une fois cliqué sur **Save**, nous pouvons nous rendre sur l'onglet **Updates** et manuellement mettre à jour les différentes règles que nous avons cochées juste avant:

Services / Snort / Update Rules

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

### Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort OpenAppID Detectors	Not Downloaded	Not Downloaded
Snort OpenAppID RULES Detectors	Not Enabled	Not Enabled

### Update Your Rule Set

Last Update

Unknown

Result: Unknown

Update Rules

Update Rules

Force Update

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

### Manage Rule Set Log

View Log

Clear Log

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size

Log file is empty

	Titre	Reference	Page	
	Mise en place de SNORT sur PFSENSE	Assurmer	7 / 8	

Une fois la mise à jour terminé, nous approchons de la fin ! Rendons-nous donc sur **Snort interfaces** pour choisir l'interface sur laquelle Snort va écouter et analyser le trafic :

The screenshot shows the PfSense web interface for the 'Edit Interface' configuration of a Snort instance. The breadcrumb trail is 'Services / Snort / Edit Interface / None'. The 'Snort Interfaces' tab is selected in the top navigation bar. Below the navigation bar, there are several tabs for different settings: 'None Settings', 'None Categories', 'None Rules', 'None Variables', 'None Preprocs', 'None Barnyard2', 'None IP Rep', and 'None Logs'. The 'General Settings' section is expanded, showing the following configuration options:

- Enable:** ☒ Enable interface
- Interface:** LAN (em1) (selected from a dropdown menu). Below the dropdown, it says: 'Choose the interface where this Snort instance will inspect traffic.'
- Description:** Interface LAN (entered in a text field). Below the text field, it says: 'Enter a meaningful description here for your reference.'
- Snap Length:** 1518 (entered in a text field). Below the text field, it says: 'Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.'

The 'Alert Settings' section is also visible, showing the following configuration options:

- Send Alerts to System Log:** ☒ Snort will send Alerts to the firewall's system log. Default is Not Checked.
- System Log Facility:** LOG\_AUTH (selected from a dropdown menu). Below the dropdown, it says: 'Select system log Facility to use for reporting. Default is LOG\_AUTH.'
- System Log Priority:** LOG\_ALERT (selected from a dropdown menu). Below the dropdown, it says: 'Select system log Priority (Level) to use for reporting. Default is LOG\_ALERT.'
- Block Offenders:** ☐ Checking this option will automatically block hosts that generate a Snort alert

Pour Assurmer nous allons demander au **PFSENSE** d'analyser le trafic de l'interface **LAN & DMZ**.

	Titre	Reference	Page	
	Mise en place de SNORT sur PFSENSE	Assumer	8 / 8	

L'avant dernière étape est d'activer toutes les règles précédemment téléchargées en nous rendant dans **LAN Categories**, sur **Snort Interfaces**, **LAN** en cochant l'option **Use IPS Policy** :

Services / Snort / Categories / LAN

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

LAN Settings LAN Categories LAN Rules LAN Variables LAN Preprocs LAN Barnyard2 LAN IP Rep LAN Logs

### Automatic Flowbit Resolution

**Resolve Flowbits** ☒ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.  
 Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

### Snort Subscriber IPS Policy Selection

**Use IPS Policy** ☒ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.  
 Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

**IPS Policy Selection** Connectivity  
 Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.

Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

On valide, et on retourne à la liste des interfaces de Snort pour cliquer sur **Start** :

Services / Snort / Interfaces

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

### Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
<input type="checkbox"/> LAN (em1)		AC-BNFA	ENABLED	DISABLED	Interface LAN	

+ Add Delete

Voilà **SNORT** est configuré sur le **PFSENSE** d'Assumer afin de prévenir d'éventuelle intrusion.